REMARKS

This application has been reviewed in light of the non-final Office Action dated 6 July 2011.

Claims 1-21 are pending in the application. Independent claims 1 and 11 have been amended to more distinctly claim the invention. The Examiner's reconsideration of the rejection in view of the following remarks is respectfully requested.

Claim Rejections under 35 U.S.C. §102(e)

Claims 1-3, 7-15 and 19-21 stand rejected under 35 U.S.C. §102(e) as being anticipated by Watson, et al. (U.S. Patent No. 7,565,678) (hereinafter 'Watson').

Watson discloses a method "for discouraging unauthorized modifications to set top boxes and gateways. ... The processor compares the resource information to the configuration information. When the resource information differs from the configuration information, then the processor detects unauthorized modifications to the set top box" (see, abstract). Watson further states, "[I]n step 308, service provider 102 can send information and operating instructions to STB 106 to reconfigure STB 106 in such a way that the modified STB 106 will again conform to the expected configuration in accordance with the data retrieved from the database" (col. 6, lines 28-34). Thus, the crux of Watson is to ensure that the configuration file is unmolested, and, if it is molested, to overwrite it with an authorized configuration file.

Watson also discloses, "[I]n addition, the operating command can also be used to allow or enable additional services..." (col. 6, lines 41-42). These 'services' can include "addressing of more HD space for extending record times or allowing extended EPG data, or allocated resources for new services, for example, electronic magazine or games and/or repartioning (sic) the fixed disk drive for more or less space for PVR or other services" (col. 6, lines 43-47). Watson also mentions, "[A]n operating instruction from service provider 102 can permit STB 106 to access additional portions of the fixed hard drive" (col. 6, line 67 to col. 7, lines 1-2). Although Watson could limit access to part of the drive, it does so only to prevent its use as a storage medium *as opposed to* preventing access to information on the non-accessible portion of the drive.

This *contrasts sharply* with the present invention. As stated in the Background section of the present application, "[H]owever, Service Providers who purchase and/or deploy these products vary greatly in their policies as to exactly what information elements they feel can be revealed to end users without compromising their companies' internal service security standards" (Page 1, lines 19-22, background). Thus, the technical problem solved by the present application is to prevent compromising of the security of the service provider, *not* maintaining a configuration of the end product or turning services on and off as disclosed in Watson.

In the present application, "[W]hen access device 102 is initially set up, information is downloaded from service provider 100, which is used to configure access device 102. This enables access device 102 to establish communication through the service provider 100 to network 101. Each access device 102 preferably includes a configuration file 104 which stores web addresses and other configuration information that permits access device 102 to connect with network 101 through service provider 100. In accordance with the present invention, service provider 100 includes a control mechanism 90, which permits the service provider to select what information elements stored in access device 102, including that derived from the configuration file 104, can be accessed by the user. In this way, the user is excluded from accessing information elements, which may be used to compromise the system security of the service provider" (Page 3, lines 25-34 and Page 4, lines 1-3).

Thus, the present application is directed to protecting the service provider's ability to provide network connections to the access device. "Service provider 100 may maintain a secured system, that is, access to service provider 100 is limited. In addition, information stored on service provider's systems may include information of a sensitive nature, which even end users need to be prevented from accessing. … Referring to FIG. 2 with continued reference to FIG. 1, service provider 100 (FIG. 1) retains control of which information elements can be revealed to an end user or subscriber; thereby enabling the service provider to maintain security over the information elements which may enable the end user to compromise the service provider system's integrity if revealed to end users" (Page 4, lines 14-32).

Claim 1 has been amended to more particularly point out the claimed invention as follows:

> *A system, comprising:*
>
> *a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network, wherein the service provider maintains a level of integrity to allow it to provide network access to an access device; and*
>
> *a control mechanism disposed at a location of the service provider which accesses each of the access devices to modify stored network connection information on a corresponding access device of a corresponding end user and thereby remotely designate portions of the information as service provider-accessible only to prevent compromise of the service provider's integrity by the corresponding end user.*

Watson does not teach the features of Claim 1. Claim 11 has been amended in a similar manner. Applicants believe that Claims 1 and 11 and their dependent claims are now in condition for allowance and request that the rejection be withdrawn and the claims be allowed to issue.

Claim Rejections under 35 U.S.C. §103(a)

Claims 4-6 and 16-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Watson in view of Benhammou, et al. U.S. Patent No. 5,991,519 (hereinafter "Benhammou").

Benhammou fails to cure the deficiencies of Watson as stated above, singly or in combination. Since claims 4-6 and 16-18 depend from independent claims 1 and 11, they contain allowable features as well. Thus, Applicants believe that claims 4-6 and 16-18 are now in condition for allowance and request that the rejection be withdrawn and the claims be allowed to issue.

In view of the foregoing, the applicants respectfully request that the rejections of the claims set forth in the Office Action of 6 July 2011 be withdrawn, that pending claims 1-21 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicant's representatives Deposit Account No. 07-0832.

Respectfully submitted,

By: ____/Jeffrey D. Hale/_______
Jeffrey D. Hale
Registration No. 40,012

Date: __7 December 2011__

Mailing Address:

Thomson Licensing LLC
2 Independence Way, Suite #200
P. O. Box 5312
Princeton, NJ 08543-5312